Nuance Management Center

Server installation and configuration guide

For:

Nuance®
Dragon® Professional
Group

Nuance®
Dragon® Legal
Group

Nuance®
Dragon®
Law Enforcement
Copyright

2017 Dragon Professional Group and Dragon Legal Group, 15.

Nuance ® Management Center.

This material may not include some last-minute technical changes and/or revisions to the software. Changes are periodically made to the information provided here. Future versions of this material will incorporate these changes.

Nuance Communications, Inc. has patents or pending patent applications covering the subject matter contained in this document. The furnishing of this document does not give you any license to such patents.

No part of this manual or software may be reproduced in any form or by any means, including, without limitation, electronic or mechanical, such as photocopying or recording, or by any information storage and retrieval systems, without the express written consent of Nuance Communications, Inc. Specifications are subject to change without notice.

Copyright © 2002-2017 Nuance Communications, Inc. All rights reserved.

Nuance, ScanSoft, the Nuance logo, the Dragon logo, Dragon, DragonBar, NaturallySpeaking, NaturallyMobile, RealSpeak, Nothing But Speech (NBS), Natural Language Technology, Select-and-Say, MouseGrid, and Vocabulary Editor are registered trademarks or trademarks of Nuance Communications, Inc. in the United States or other countries. All other names and trademarks referenced herein are trademarks of Nuance Communications or their respective owners. Designations used by third-party manufacturers and sellers to distinguish their products may be claimed as trademarks by those third-parties.

Disclaimer

Nuance makes no warranty, express or implied, with respect to the quality, reliability, currentness, accuracy, or freedom from error of this document or the product or products referred to herein and specifically disclaims any implied warranties, including, without limitation, any implied warranty of merchantability, fitness for any particular purpose, or noninfringement.

Nuance disclaims all liability for any direct, indirect, incidental, consequential, special, or exemplary damages resulting from the use of the information in this document. Mention of any product not manufactured by Nuance does not constitute an endorsement by Nuance of that product.

Notice

Nuance Communications, Inc. is strongly committed to creating high quality voice and data management products that, when used in conjunction with your own company’s security policies and practices, deliver an efficient and secure means of managing confidential information.

Nuance believes that data security is best maintained by limiting access to various types of information to authorized users only. Although no software product can completely guarantee against security failure, Dragon software contains configurable password features that, when used properly, provide a high degree of protection.

We strongly urge current owners of Nuance products that include optional system password features to verify that these features are enabled! You can call our support line if you need assistance in setting up passwords correctly or in verifying your existing security settings.

Published by Nuance Communications, Inc., Burlington, Massachusetts, USA


6/9/2017
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dragon_NMCInstallGuideCover_20160929_v4</td>
<td>1</td>
</tr>
<tr>
<td>About this guide</td>
<td>iv</td>
</tr>
<tr>
<td>Guide overview</td>
<td>v</td>
</tr>
<tr>
<td>Audience</td>
<td>v</td>
</tr>
<tr>
<td>Additional resources</td>
<td>vi</td>
</tr>
<tr>
<td>Documentation</td>
<td>vi</td>
</tr>
<tr>
<td>Training</td>
<td>vii</td>
</tr>
<tr>
<td>Support</td>
<td>vii</td>
</tr>
<tr>
<td>Chapter 1: Introduction</td>
<td>1</td>
</tr>
<tr>
<td>About Nuance Management Center</td>
<td>2</td>
</tr>
<tr>
<td>Physical architecture</td>
<td>3</td>
</tr>
<tr>
<td>Chapter 2: Installation checklist</td>
<td>4</td>
</tr>
<tr>
<td>Checklist—Planning the server installation</td>
<td>5</td>
</tr>
<tr>
<td>Chapter 3: Preparing for your server installation</td>
<td>6</td>
</tr>
<tr>
<td>Software requirements—Server</td>
<td>7</td>
</tr>
<tr>
<td>Application server and database server</td>
<td>7</td>
</tr>
<tr>
<td>NMC console</td>
<td>8</td>
</tr>
<tr>
<td>Hardware requirements—Server</td>
<td>9</td>
</tr>
<tr>
<td>Server installation prerequisites</td>
<td>10</td>
</tr>
<tr>
<td>Application server and database server</td>
<td>10</td>
</tr>
<tr>
<td>NMC console</td>
<td>10</td>
</tr>
<tr>
<td>Other considerations</td>
<td>11</td>
</tr>
<tr>
<td>Network bandwidth recommendations</td>
<td>11</td>
</tr>
<tr>
<td>Excluding files and folders from anti-virus protection</td>
<td>11</td>
</tr>
<tr>
<td>Using a network traffic switch</td>
<td>11</td>
</tr>
<tr>
<td>Obtaining required server software</td>
<td>13</td>
</tr>
<tr>
<td>Opening required ports</td>
<td>14</td>
</tr>
<tr>
<td>Chapter 4: Installing the servers</td>
<td>15</td>
</tr>
<tr>
<td>Installing SQL Server</td>
<td>16</td>
</tr>
<tr>
<td>Installing Nuance Management Center</td>
<td>17</td>
</tr>
<tr>
<td>Chapter 5: Post-installation tasks</td>
<td>23</td>
</tr>
<tr>
<td>Installing and binding the SSL certificate</td>
<td>24</td>
</tr>
</tbody>
</table>
About certificates ............................................................................................................... 24
Install the SSL certificate—Installing on the server .......................................................... 24
Install the SSL certificate—Installing on a load balancing switch .................................. 27
Testing and troubleshooting your SSL configuration ....................................................... 27
Verifying the NMS Platform service is running ............................................................... 29
Starting the NMS Platform service manually .................................................................. 29
Configuring your network switch .................................................................................... 30
Logging in to the Nuance Management Center (NMC) console ..................................... 31
Determining your database backup method ...................................................................... 32
Configuring the Dragon client for use with Nuance Management Center ....................... 33

Chapter 6: Preparing for your Active Directory single sign-on configuration ....................... 34
Single sign-on overview ..................................................................................................... 35
Before you begin ................................................................................................................ 36
Software requirements—Single sign-on for the Cloud NMC server ................................. 36
Other requirements .......................................................................................................... 36
Checklist—Planning the single sign-on setup .................................................................. 36
Creating an NMC console Administrator user for Active Directory .............................. 38
Setting the Active Directory connection string ............................................................... 39
Creating and configuring user accounts for single sign-on .............................................. 40
Creating user accounts .................................................................................................. 40
Configuring user accounts .............................................................................................. 40

Chapter 7: Installing the Local Authenticator ................................................................... 41
About the Local Authenticator .......................................................................................... 42
Local Authenticator logs .................................................................................................. 42
Downloading the Local Authenticator .............................................................................. 43
Creating organization tokens ........................................................................................... 44
Installing and binding the SSL certificate ......................................................................... 45
About signed certificates .................................................................................................. 45
Install the SSL certificate ................................................................................................. 45
Testing and troubleshooting your SSL configuration ....................................................... 48
Installing the Local Authenticator ..................................................................................... 50
Editing the configuration file ............................................................................................ 54
Starting the Local Authenticator service ......................................................................... 55

Appendix A: Database backups ....................................................................................... 56
About database backups ................................................................................................... 57
Disabling automatic database backups ........................................................................... 57
About this guide

Guide overview ................................................................. v
Audience ................................................................................. v
Additional resources ............................................................... vi
  Documentation ........................................................................ vi
  Training ............................................................................... vii
  Support ............................................................................... vii
Guide overview

The Nuance Management Center Server Installation and Configuration Guide provides the following:

- Installation and configuration instructions for on-premise Nuance Management Center (NMC) servers.
- Configuration instructions for single sign-on authentication.

This guide contains installation and configuration instructions for on-premise NMC servers. It also contains instructions for configuring single-sign-on authentication, which you can implement regardless of whether you are hosting your own NMC server on-premise or using Nuance’s hosted NMC server in the cloud. Use the following table to determine the chapters that are applicable to you:

<table>
<thead>
<tr>
<th>NMC server type</th>
<th>Applicable chapters</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-premise</td>
<td>All, except chapter 7</td>
</tr>
<tr>
<td>Nuance-hosted</td>
<td>1, 6, 7</td>
</tr>
</tbody>
</table>

**Note:** This guide describes only the NMC server installation. When you have completed the NMC server installation, you must then install Dragon clients and configure them for Nuance Management Center. For Dragon client installation and configuration, see the Dragon Installation Guide.

Audience

This guide is intended for IT administrators, database administrators, and Dragon administrators whose responsibility is to perform the following:

- Install and configure an on-premise NMC server.
- Set up and manage single sign-on user authentication.
- Install and manage a SQL Server database.

This guide assumes you have experience in hardware configuration, software installation, database management, and networking.
Additional resources

The following resources are available in addition to this guide to help you manage your Dragon installation.

### Documentation

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dragon Group Citrix Administrator Guide</strong></td>
<td>Hardware, software, and network requirements for deploying Dragon in a network of client computers that connect to a Citrix server to access published applications.</td>
<td>Dragon Support web site</td>
</tr>
<tr>
<td><strong>Nuance Management Center Administrator Guide</strong></td>
<td>Information on creating and maintaining objects and managing Dragon clients from the Nuance Management Center (NMC) console.</td>
<td>Dragon Support web site</td>
</tr>
<tr>
<td><strong>Nuance Management Center Help</strong></td>
<td>Instructions for configuring and managing the Nuance Management Center (NMC) console and Dragon clients.</td>
<td>When Nuance Management Center is open, click the NMC console Help button.</td>
</tr>
<tr>
<td><strong>Dragon client Help</strong></td>
<td>Commands and instructions for dictating, correcting, and more with the Dragon client.</td>
<td>When Dragon is open, click the Help icon on the DragonBar, and then select Help Topics.</td>
</tr>
<tr>
<td><strong>Dragon Release Notes</strong></td>
<td>New features, system requirements, client upgrade instructions, and known issues.</td>
<td>Dragon Help. Do the following:</td>
</tr>
<tr>
<td></td>
<td>1. When Dragon is open, click the Help icon on the DragonBar, and then select Help Topics.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Get started</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Dragon</strong></td>
<td></td>
</tr>
</tbody>
</table>
Training

Nuance provides several Dragon training offerings, like webinars, demos, and Nuance University online training courses. For more information, see the Dragon Support web site.

Support

The Dragon Support web site provides many resources to assist you with your Dragon installation, like forums and a searchable knowledgebase. For more information on Support offerings, see the Dragon Support web site at:

Chapter 1: Introduction

About Nuance Management Center ................................................................. 2
Physical architecture ....................................................................................... 3
About Nuance Management Center

Nuance Management Center allows Dragon administrators to manage all Dragon Group clients from a single central console. The console, called the Nuance Management Center (NMC) console, allows you to do the following:

- Configure options for clients at the site and group level
- Centrally manage your Dragon product licensing
- Share data, like words and auto-text commands, with Dragon clients and across other Nuance products
- Audit user session events
- Monitor client usage and trends through reporting

Nuance Management Center installs on a server. You can choose to install, configure, and maintain your own on-premise NMC server, or you can use the Nuance-hosted server in the cloud.

Using Nuance Management Center with your Dragon installation is an optional feature that you enable in Dragon.
Physical architecture

The physical configuration of Nuance Management Center includes:

- **Application server**—The NMC server. Stores user accounts, settings, and administrative information. Can be a single machine, or, in large installations, can be multiple servers load-balanced by a network traffic switch. Can be the Nuance-hosted NMC server in the cloud, or a server that you install and host on-premise.

- **Database server**—Hosts the SQL database that stores your data, like sites, groups, and licenses. Can be the same physical machine as your application server, or a separate database server.

- **Dragon clients**—Client computers with Dragon installed.

If you choose to host your own NMC server on-premise, there are two configuration options:

- **Single-tier**—Your application server and database server are located on the same physical machine.

- **Two-tier**—Your application server and database server run on separate machines.

If you’re hosting your own NMC server, the installation process installs the NMC server, database server, and NMC console from a single executable file. During the installation, you can choose the location of your database server.
Chapter 2: Installation checklist

Checklist—Planning the server installation .......................................................... 5
## Checklist—Planning the server installation

If you are installing and managing your own Nuance Management Center (NMC) server and database server on-premise, use this checklist to help you prepare for the installation.

When you finish installing the server, see the *Nuance Management Center Administrator Guide* for the NMC console setup checklist. You must also install Dragon clients if you are a new Dragon customer.

<table>
<thead>
<tr>
<th>Server</th>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>NMC server and database server</td>
<td>Ensure all system requirements have been met.</td>
<td>“Software requirements—Server” on page 7</td>
</tr>
<tr>
<td>NMC server and database server</td>
<td>Ensure all prerequisites have been met.</td>
<td>“Server installation prerequisites” on page 10</td>
</tr>
<tr>
<td>NMC server</td>
<td>Obtain the required server software.</td>
<td>“Obtaining required server software” on page 13</td>
</tr>
<tr>
<td>NMC server and database server</td>
<td>Ensure required ports are open.</td>
<td>“Opening required ports” on page 14</td>
</tr>
<tr>
<td>Database server</td>
<td>Install the SSL certificate.</td>
<td>“Installing and binding the SSL certificate” on page 24</td>
</tr>
<tr>
<td>NMC server and database server</td>
<td>Install the required software.</td>
<td>“Installing SQL Server” on page 16</td>
</tr>
<tr>
<td>NMC server</td>
<td>Run the NMS_SuiteInstaller.exe file to install the NMC server, NMC console, and database.</td>
<td>“Installing Nuance Management Center” on page 17</td>
</tr>
<tr>
<td>NMC server</td>
<td>If you’re using multiple NMC servers, configure your network traffic switch.</td>
<td>“Configuring your network switch” on page 30</td>
</tr>
<tr>
<td>NMC server</td>
<td>Verify that the NMS Platform service is running.</td>
<td>“Verifying the NMS Platform service is running” on page 29</td>
</tr>
<tr>
<td>NMC server</td>
<td>Log in to the NMC console. If you’re using a network traffic switch, ensure you access the NMC console using the name or address of the switch in the URL.</td>
<td>“Logging in to the Nuance Management Center (NMC) console” on page 31</td>
</tr>
<tr>
<td>Database server</td>
<td>Determine your database backup method.</td>
<td>“Determining your database backup method” on page 32</td>
</tr>
</tbody>
</table>
Chapter 3: Preparing for your server installation

Software requirements—Server ................................................................. 7
  Application server and database server ............................................. 7
  NMC console .................................................................................. 8
Hardware requirements—Server ............................................................ 9
Server installation prerequisites ............................................................. 10
  Application server and database server ............................................. 10
  NMC console .................................................................................. 10
Other considerations ........................................................................... 11
  Network bandwidth recommendations .............................................. 11
  Excluding files and folders from anti-virus protection ...................... 11
  Using a network traffic switch ......................................................... 11
Obtaining required server software ..................................................... 13
Opening required ports ....................................................................... 14
Software requirements—Server

If you’re hosting your own Nuance Management Center (NMC) server and database server on-premise, you must first download the Nuance Management Center installation package. When you purchase Nuance Management Center, Nuance sends you an email with a link to download the package. You must then ensure that your servers meet the following software requirements.

Application server and database server

The following table provides software requirements for the following scenarios:

- Your application server and database server are separate physical machines.
- Your application server and database server are on the same physical machine.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Application server</th>
<th>Database server</th>
<th>Combined application and database server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>One of the following:</td>
<td>One of the following:</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>- Microsoft® Windows Server 2008 R2, Service Pack 1, Service Pack 2</td>
<td>- Microsoft® Windows Server 2008 R2, Service Pack 2, Service Pack 1, Service Pack 2</td>
<td>- Microsoft® Windows Server 2008 R2, Service Pack 1, Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>- Microsoft® Windows Server 2012 R2 (64 bit)</td>
<td>- Microsoft® Windows Server 2012 R2 (64 bit)</td>
<td>- Microsoft® Windows Server 2012 R2 (64 bit)</td>
</tr>
<tr>
<td></td>
<td>Ensure you have all current service packs installed.</td>
<td>Ensure you have all current service packs installed.</td>
<td>Ensure you have all current service packs installed.</td>
</tr>
</tbody>
</table>
### Chapter 3: Preparing for your server installation

<table>
<thead>
<tr>
<th>Feature</th>
<th>Application server</th>
<th>Database server</th>
<th>Combined application and database server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows components</strong></td>
<td>• Microsoft .NET Framework 4.5.2 or later, including the ASP .NET component&lt;br&gt;• Internet Information Services (IIS) 7, 7.5, or 8.0</td>
<td>None.</td>
<td>• Microsoft .NET Framework 4.5.2 or later, including the ASP .NET component&lt;br&gt;• Internet Information Services (IIS) 7, 7.5, or 8.0</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>• SSL certificate&lt;br&gt;While Nuance Management Center supports self-signed certificates, Nuance strongly recommends that you use a certificate signed by a certificate authority.&lt;br&gt;For more information on SSL certificates, see &quot;Installing and binding the SSL certificate&quot; on page 24.</td>
<td>None.</td>
<td>• SSL certificate&lt;br&gt;While Nuance Management Center supports self-signed certificates, Nuance strongly recommends that you use a certificate signed by a certificate authority.&lt;br&gt;For more information on SSL certificates, see &quot;Installing and binding the SSL certificate&quot; on page 24.</td>
</tr>
</tbody>
</table>

### NMC console

- Microsoft Internet Explorer 10 or 11, or latest version of Chrome
- Microsoft .NET Framework 4.5.2 or later
Hardware requirements—Server

If you’re hosting your own Nuance Management Center (NMC) server and database server on-premise, ensure the servers meet the following hardware requirements.

For every 1,000 users:

- One Quad-Core physical server to host the SQL database, NMC server, and NMC console
  - **Processor**: Quad-Core 2 GHz CPU
  - **Minimum RAM**: 4 GB recommended
  - **Core Application Disk Storage**: 40 GB for the NMC server

- **If using Roaming user profiles**: A server, separate machine, or RAID array to host the Master user profiles directory
  - **Processor**: Intel® Pentium 4® or later, or AMD Athlon 64 or later
    - **CPU**: 1 GHz minimum (2.4 GHz recommended)
    - **RAM**: 4 GB
    - **Cache**: 512 KB minimum L2 Cache (1 MB recommended)

- One Database Server
  - **Processor**: Dual-Core 2GHz CPU
  - **Minimum RAM**: 4 GB
Server installation prerequisites

In addition to the system requirements, you'll also need the following.

Application server and database server

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Server</th>
<th>Additional Information</th>
</tr>
</thead>
</table>
| Windows administrator account        | Application                     | All services should run under this account. This account must also meet the following requirements:  
                                             |                                 | - Is an administrator account in the workgroup (single-tier) or in the domain (two-tier)  
                                             |                                 | - Account and password never expire  
                                             |                                 | - Has rights to install software  
                                             |                                 | - Has rights to install, create, and start a Windows service  
                                             |                                 | - Has full read/write access to the database server, and to all servers in the network  
                                             |                                 | You provide this account name and password during the server installation.  
                                             |                                 | **To allow this account to launch the services upon installation completion, you must set it up with** **Log on as Service** rights. |
| Computer name or IP address of your server | Application and database | Must be provided during the NMC server installation.                                      |
| Directory permissions                | Application and database        | Assign full read/write/modify permissions to the directories where the NMC server, NMC console, and database server are installed. |

NMC console

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full trust privileges</td>
<td>None.</td>
</tr>
</tbody>
</table>
Other considerations

Consider the following while you prepare for your NMC server installation.

Network bandwidth recommendations

Nuance recommends the following network bandwidth speeds for Nuance Management Center.

<table>
<thead>
<tr>
<th>Number of clients</th>
<th>Minimum network speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>&gt;100</td>
<td>100 Mbps</td>
</tr>
</tbody>
</table>

Excluding files and folders from anti-virus protection

If you have anti-virus software installed on your application and database servers and Dragon clients, you should exclude the following files and folders from the anti-virus scan to ensure optimum performance.

Servers

- Nuance folder and all sub-folders
- **File extensions**: DAT, DRA, ENH, INI, LCK, LOG, NWV, SIG, TXT, USR, VER, VOC, WAV

Clients

- C:\Program Files\Nuance folder and all sub-folders
- C:\Program Data\Nuance folder and all sub-folders
- C:\<windows user ID>\AppData folder and all sub-folders
- C:\Documents and Settings\All Users\Application Data\Nuance folder and all sub-folders
- C:\Documents and Settings\<Windows user ID>\Local Settings\Temp folder
- **File extensions**: BD, BIN, DAT, DVC, ENH, GSB, GRM, GRX, INI, LCK, NWV, SIG, SVC, USR, VER, VOC, WAV, XML, LOG

Using a network traffic switch

If you have a large organization and you're implementing more than one NMC server, you can include a network traffic switch in your network to balance the load on the servers.

The following table describes the recommended settings for your device.

<table>
<thead>
<tr>
<th>Component</th>
<th>Setting</th>
</tr>
</thead>
</table>
| Network Interface Card (NIC)—Gigabit cards | Automatic.  
Switches and gigabit cards must have the same setting. |
| Network Interface Card (NIC)—10/100Mb cards | Network link speed and duplex must be set the same on all servers, workstations, and other network equipment, or performance and recognition degradation could occur. |
| Network speed—10 Mbps              | Full Duplex                                                             |
### Component | Setting
---|---
Network speed—100 Mbps | Full Duplex
Obtaining required server software

The following server software is required. You can obtain all software from microsoft.com.

- Microsoft .NET Framework 4.5
- One of the following:
  - Microsoft® Windows Server 2008, Service Pack 1, Service Pack 2
  - Microsoft® Windows Server 2008 R2, 32-bit and 64-bit
  - Microsoft® Windows Server 2008 R2 64 bit Service Pack 2
  - Microsoft® Windows Server 2012
  - Microsoft® Windows Server 2012 R2 (64 bit)
## Opening required ports

You must open the following ports to allow communication between components.

<table>
<thead>
<tr>
<th>Port</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>389 TCP</td>
<td>NMC server</td>
<td>Allows communication between the NMC server and your Active Directory, if you are using single sign-on authentication.</td>
</tr>
<tr>
<td>443</td>
<td>NMC server</td>
<td>Allows communication between Dragon clients and the NMC server. Also allows communication between NMC console workstations and the NMC server.</td>
</tr>
<tr>
<td>1433 Custom</td>
<td>Database server</td>
<td>Allows communication between the NMC server and the database server if they are on separate physical machines.</td>
</tr>
</tbody>
</table>
Chapter 4: Installing the servers

Installing SQL Server ................................................................. 16
Installing Nuance Management Center .................................. 17
Installing SQL Server

Use the following settings during your installation:

1. On the Feature Selection screen, select the following features:
   - Database Engine Services
   - Management Tools – Basic
   - Management Tools – Complete

While using Nuance Management Center does not require you to install Analysis Services and Reporting Services, these services may help Nuance technical support troubleshoot any issues that occur with your installation or database.

2. On the Instance Configuration screen, leave the Default instance option selected.

3. On the Server Configuration screen, click Use the same account for all SQL Server Services.
   1. Enter the username and password of the Windows user account that the SQL Server services should all run under. Use the same account that the product services will run under.

   If you are planning to install the database and all Dragon servers on a single machine, Nuance recommends using an account in a workgroup. Enter the account in the format “Domain\User_Name.”

   2. Enter the password that other servers and clients on the Dragon network will use to access the database.

4. On the Database Engine Configuration screen:
   - Nuance recommends using Windows Authentication Mode for most networks.
   - Add at least three user accounts to administer the SQL database, including the account you created to run all NMS services.

5. On the Reporting Services Configuration screen, select Install the native mode default configuration.

6. If the Complete with failures screen appears, save the log to a location where you can retrieve it. The Nuance support team can use this log file if any network issues arise.
Installing Nuance Management Center

You install all the components of the NMC server on the same machine using a single installation wizard. After the installation is complete, use the console to configure the server.

Caution:

Even if you do not want to store the data files in SQL Server’s default location, allow the installer to create the database, its transaction log, and its dump device in the default location. When the installation is complete, you can move the database and its files to a different location.

**ADVANCED INSTALLERS ONLY:** Alternatively, create the NuanceMC.mdf database, the NuanceMC_log.LDF transaction log, and the NuanceMCDump.bak dump device on your server before installing the NMC server.

1. On the NMC server (for single-node installations) or each node (for multiple-node installations), run NMS_SuiteInstaller.exe.
   The Choose Setup Language screen of the InstallShield Wizard opens.
2. Select a language from the drop-down list.
3. Click Next until you reach the License Agreement screen.
4. Accept the license agreement, and then click Install.

The wizard installs several components of the NMS Suite, then the Customer Information screen appears:

5. Enter a user name and company name, and then click Next.
The **Choose Destination Location** screen appears:

6. Choose where you want to install the NMS platform (default recommended), and then click **Next**.

The **Setup Type** screen appears:

7. Choose a setup configuration:
   - **Single-node installations**: Select *On a server with an SSL certificate installed directly on that server*.
   - **Multiple-node installations**: Select *Behind a networking device with an SSL certificate installed*.

8. Click **Next**.
The wizard installs NMS Suite components. When it is finished, the **Database Server** screen appears:

9. **Enter the required database information:**
   
   1. Enter the machine name or IP address of the physical server where you have installed the SQL Database Server software. The wizard creates the database and its backup directory in default locations on that server automatically.
   
   2. Under **Connect using**, select a method of validating connections to the server:
      
      - **Windows authentication**: Use a Windows login and password to authorize access.
      - **SQL Server authentication**: Use a SQL Server login and password.

      Choose the same type of authentication for access to the database that you chose when you installed the SQL Server. Nuance recommends using Windows authentication.

   3. **SQL Server authentication only**: Enter the database system administrator login name and password that you set up in the SQL Server into the **Login ID** and **Password** text boxes provided.

      These fields are not used for Windows authentication.

10. **Click Next.**
The wizard installs several NMS Suite components. When it is finished, the **Organization Id** screen appears:

11. Enter the unique ID that Nuance assigned to your organization. You should have received this ID with your Dragon software package.

   Later, you can access your organization ID in the NMC console. For more information on organization IDs, see the *Nuance Management Center Administrator Guide*.

12. Click **Next**.

   The **Enter new password for NMC** screen appears:

   13. Enter a password for the default administrator account.
Chapter 4: Installing the servers

The first time you log into the NMC console, use the “admin” login ID with the password you created in this step.

14. Click **Next**.

The **Setup Type** screen appears:

![Setup Type Screen]

15. Select the account type under which NMS windows service will run, and then click **Next**.

The **Service logon** screen appears:

![Service logon Screen]

16. Enter the user name and password of the Windows user account under which NMS will run, then click **Next**.
The install wizard installs several components, then opens the **Choose Destination Location** screen for the **NMC – InstallShield Wizard**:

17. Choose where you want the install wizard to install the NMC console (default recommended), and then click **Next**.

   The wizard installs the NMC console.

18. When the installation is complete, click **Finish**.

19. If the Windows Server 2008, 2012, or 2012 R2 firewall was turned on during the installation, you must now open port 443 so that the NMC console can communicate with the NMS platform.

20. Import your license key in the NMC console:
   1. In a supported browser, go to https://<servername>/nmchtml/.
   2. Log into the NMC console using the "admin" ID and the password you entered in the setup process.
   3. In the **Licensing** ribbon, click **Import License Key**.
   4. Enter your license key.

   For more information on license keys, see the *Nuance Management Center Administrator Guide*. 
Chapter 5: Post-installation tasks

Installing and binding the SSL certificate

1. About certificates
2. Install the SSL certificate—Installing on the server
3. Install the SSL certificate—Installing on a load balancing switch
4. Testing and troubleshooting your SSL configuration

Verifying the NMS Platform service is running

1. Starting the NMS Platform service manually

Configuring your network switch

Logging in to the Nuance Management Center (NMC) console

Determining your database backup method

Configuring the Dragon client for use with Nuance Management Center
Installing and binding the SSL certificate

About certificates

Using SSL requires that you obtain an SSL certificate. Nuance Management Center supports both signed certificates from a certificate authority, and self-signed (or internally generated) certificates. However, Nuance strongly recommends that you use a signed certificate, as self-signed certificates are not always easily recognized by the client the same way signed certificates are.

You can obtain signed certificates from certificate authorities, such as GoDaddy or Verisign. The certificate authority must be a trusted authority known to both the client computer and the server. To obtain a signed certificate, you’ll need to provide information to the certificate authority about your organization and the server on which you are installing the certificate in the Certificate Signing Request (CSR). Each certificate authority may require different information. Typically, the information can include the following:

- Organization name
- Organization location information, such as town and state
- Computer name for the server on which you are installing the certificate
- Extended Key Usage value, such as 2.5.29.37. Extended key usage further refines key usage extensions, which define the purpose of the public key contained in the certificate.
- Key Size, such as 2048 bits or 4096 bits. Determines the length of the public key in the certificate. A longer key provides stronger security. You determine the level of security that is appropriate for your environment.

You obtain this information from your IT department, or from the person who installed and configured your server.

For more detailed information on installing SSL certificates, see:


Install the SSL certificate—Installing on the server

Clients contact the Local Authenticator on the standard HTTP ports 80 and 443.

1. Install an SSL certificate in the Personal Store under the Local Computer section for the "logon as" user account under which the NMS service is running.

   To add the Certificates Snap-in and view the certificates installed on the local computer, see https://technet.microsoft.com/en-us/library/cc754431(v=ws.11).aspx.
2. Note the subject of the certificate.

This should match the computer name that the certificate is deployed on, or be a wildcard. This must match exactly the host used in the endpoints. For information on viewing the subject, see https://technet.microsoft.com/en-us/library/cc754686(v=ws.10).aspx.
3. Copy the thumbprint of the certificate. You use the thumbprint to bind the certificate to the port used by the primary NMS services in the next step.

For information on retrieving the thumbprint, see https://msdn.microsoft.com/en-us/library/ms734695.aspx.

4. Bind the SSL port (443) used by the services to the certificate.

   **Windows Server 2008 or 2012:**
   
   a. Open a command prompt.
   
   b. Using the netsh utility, run the following command to bind port 443 to the certificate:

   ```
   netsh http add sslcert ipport=0.0.0.0:443 certhash=<thumbprint> appid=
   {00000000-0000-0000-0000-000000000000}
   ```

5. Verify that the UseSSL setting is set to true (this should have been done by the installer):

   a. In `Nuance.NMS.Server.exe.config`, located in the NMS Platform installation folder, find the line near the top that contains the key="UseSSL" tag.

   b. Change the value to true:

   ```
   <add key="UseSSL" value="true"/>
   ```

6. Bind the SSL certificate under IIS to port 443.
a. In the IIS Manager, from the left panel, click **Default Web Site**.
b. From the right panel, click **Bindings**....
   The Site Bindings dialog box opens.
c. Click **Add**.
   The Add Site Binding dialog box opens.
d. From the **Type** drop-down list, select **https**.
e. From the **SSL certificate** drop-down list, select the certificate that you installed.
f. Click **OK**.
   The Site Bindings dialog box appears. Ensure that the binding is displayed correctly.
7. Restart the NMS Platform server to allow any configuration changes to take effect.

Install the SSL certificate—Installing on a load balancing switch

Nuance uses this mode in the Nuance data center when the NMC server is behind a load balancing switch that also decrypts SSL. In this scenario, the load balancing switch would strip the SSL encryption and forward the messages on to the appropriate NMC server. Inside the firewall, these messages would be unencrypted, and the NMC server would receive them as HTTP with no SSL encryption.

This should only be configured by experienced networking personnel. It requires in-depth knowledge about load-balancing switches, which is outside the scope of this guide.

1. Verify that UseSSL is set to false (this should have been done by the installer):
   a. In **Nuance.NMS.Server.exe.config**, located in the NMC Platform installation folder, find the line near the top that contains the key="UseSSL" tag.
   b. Change the value to false:
      
      ```xml
      <add key="UseSSL" value="false"/>
      ```
2. Restart the NMC server to allow the configuration changes to take effect.

Testing and troubleshooting your SSL configuration

Run these tests on a different computer. Do not run them on the NMC server.

Use the browser

1. Can you access and log into the NMC console?
   a. Connect to https://<SERVER_NAME>/NMCHTML/.
      If you see the Nuance Management Center login page, port 443 is working, and the NMC console is being deployed properly.
   b. Log in to the NMC console. If successful, the console is able to communicate with the server.
2. Can you access the NMC console status interface?
      An XML response should appear in the browser.
3. Can you make RESTful web service calls?
Attempt to create an NMS session using the browser.


   A prompt for a login and password appears.

b. Use any valid NMC console login and password.

c. If some XML is returned, the NMC console is configured properly and working with SSL.

4. Can you access the NMS API Help pages?


2. Enter any credentials if prompted.

3. An HTML page with help for one of the NMS API sets should appear. If you see this help, the NMC server is configured and working properly.

Check the Bindings

If the NMC console is not working, make sure that the ports are properly bound to the SSL certificate. You can do this by using the "netsh http show sslcrt" command to display the current configuration. Be sure that port 443 is bound to the certificate.
Verifying the NMS Platform service is running

When the installation completes, the NMS Platform service starts automatically if the Windows administrator account under which it is running has the correct privileges. Post-installation, you should verify that the service is running.

To verify, check the Services dialog box on the physical NMC server. If the service is not running, you must start it manually.

Starting the NMS Platform service manually

Before starting the service manually, verify that the Windows administrator account has the correct privileges. For more information, see “Server installation prerequisites” on page 10.

If the account has the correct privileges, do the following to start the service manually:

1. Open the Windows Control Panel.
2. Click Administrative Tools.
4. Locate the NMS Platform service, and then right-click the service and select Properties. The NMS Platform Properties dialog box opens.
5. From the Startup type drop-down list, select Automatic.
6. Click the Start button to start the service.
7. Click OK. The dialog box closes.
Configuring your network switch

If you have multiple NMC servers in your environment, you can use a network traffic switch to balance the incoming client activity among your servers. You can configure the switch to make an API call periodically to your servers to ensure they are operational.

Configure the switch to make the following API call:

http://<NMS-Server-Name>:443/Nuance.NMS.Services/NMSServiceStatus/Rest/Status

If operational, the NMC servers return the following XML response:

```xml
  <Status>Running</Status>
  <ServerDateTimeUTC>2010-12-13T20:50:13.0969590Z</ServerDateTimeUTC>
  <InterfaceType>basicHttpTransport</InterfaceType>
</ServiceStatusResponse>
```

If the servers are down, the switch receives an error. If the switch receives anything other than the expected response, the switch can tag a specific server as down and reroute network traffic.
Logging in to the Nuance Management Center (NMC) console

Ensure you can log in to the NMC console using the administrator login and password.

If you have multiple NMC servers in your environment and you are using a network traffic switch to balance the load, ensure you substitute the name or IP address of the switch for the NMC server name in the URL when you access the NMC console.

1. Open a browser.
2. Enter the NMC console URL in the address bar.
   
   You should have received this address in your welcome email from Nuance. The URL is in the format: https://<servername>/nmchtml

3. Enter the following information:
   
   **User Name**: admin
   
   **Password**: The password you specified for the administrator account during the installation.

4. Click **Login**.

   The NMC console opens.
Determining your database backup method

The NMC server schedules database backups automatically. However, you can choose to manage database backups yourself and disable the automatic backups. You should determine your database backup method before users begin regular Nuance Management Center use.

For more information on Nuance Management Center database backups, see “About database backups” on page 57.
Chapter 5: Post-installation tasks

Configuring the Dragon client for use with Nuance Management Center

When you have finished the NMC server installation and configuration, you must install Dragon clients if you have not already done so, and then configure the Dragon clients for use with Nuance Management Center.

If you are a Nuance Management Center Standalone customer and you want to enable NMS mode, you must also configure your Dragon clients for use with Nuance Management Center.

For more information on configuring Dragon clients for use with Nuance Management Center, see the *Dragon Installation Guide*. 
Chapter 6: Preparing for your Active Directory single sign-on configuration

Single sign-on overview .................................................................................................................. 35
Before you begin ............................................................................................................................ 36
  Software requirements—Single sign-on for the Cloud NMC server ........................................ 36
  Other requirements .................................................................................................................... 36
  Checklist—Planning the single sign-on setup ....................................................................... 36
Creating an NMC console Administrator user for Active Directory ............................................ 38
Setting the Active Directory connection string ......................................................................... 39
Creating and configuring user accounts for single sign-on ............................................................ 40
  Creating user accounts ........................................................................................................ 40
  Configuring user accounts .................................................................................................... 40
Single sign-on overview

You can optionally implement Active Directory single sign-on authentication rather than using the native Nuance Management Center authentication, which requires a separate login and password. With single sign-on, users can simply use their Windows login and password to access the Dragon client and other applications.

Ideally, you should decide to use single sign-on before you install Dragon clients, as you can configure some of the required settings during the batch or push install. However, it is possible to enable single sign-on after client installation.

Both on-premise customers and customers using the Nuance-hosted cloud server can implement single sign-on.
Before you begin

Review the following before beginning your single sign-on configuration.

Software requirements—Single sign-on for the Cloud NMC server

Cloud NMC server

If you are using the Nuance-hosted NMC server and you want to implement single sign-on, you must install the Local Authenticator on a server with the following:

- Latest version of the Microsoft .NET Framework installed
- One of the following operating systems:
  - Microsoft® Windows Server 2008 R2, Service Pack 1, Service Pack 2
  - Microsoft® Windows Server 2008 R2, 32-bit and 64-bit
  - Microsoft® Windows Server 2008 R2 64 bit Service Pack 2
  - Microsoft® Windows Server 2012
  - Microsoft® Windows Server 2012 R2 (64 bit)

In addition, you'll need the following:

- SSL certificate
  While Nuance Management Center supports self-signed certificates, Nuance strongly recommends that you use a certificate signed by a certificate authority. For more information, see “Installing and binding the SSL certificate” on page 45.

You can download the Local Authenticator installation file from the NMC console.

For information on which server to install the Local Authenticator, see “About the Local Authenticator” on page 42.

Other requirements

- When you create user accounts in the NMC console, each user’s login must match that user’s Windows Domain login exactly.
  For more information on creating user accounts, see the Nuance Management Center Administrator Guide.

Checklist—Planning the single sign-on setup

If you’re using single sign-on authentication, use these checklists to help you prepare for the configuration.

Cloud NMC server

If you’re using the Nuance-hosted cloud NMC server, use this checklist to help you prepare for the configuration.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Review software requirements</td>
<td>“Software requirements—Single sign-on for the Cloud NMC server” on page 36</td>
</tr>
<tr>
<td>☐ Create an NMC console administrator account for Active Directory</td>
<td>“Creating an NMC console Administrator user for Active Directory” on page 38</td>
</tr>
<tr>
<td>Task</td>
<td>Reference</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Directory</td>
<td><strong>Set the Active Directory connection string</strong> on page 39</td>
</tr>
<tr>
<td></td>
<td><strong>Create and configure user accounts in the NMC console</strong> on page 40</td>
</tr>
<tr>
<td></td>
<td><strong>Download the Local Authenticator</strong> on page 43</td>
</tr>
<tr>
<td></td>
<td><strong>Create an organization token</strong> on page 44</td>
</tr>
<tr>
<td></td>
<td><strong>Install and bind the SSL certificate on the Local Authenticator server</strong> on page 45</td>
</tr>
<tr>
<td></td>
<td><strong>Install the Local Authenticator</strong> on page 50</td>
</tr>
<tr>
<td></td>
<td><strong>Edit the Local Authenticator configuration file</strong> on page 54</td>
</tr>
<tr>
<td></td>
<td><strong>Start the Local Authenticator service</strong> on page 55</td>
</tr>
<tr>
<td></td>
<td><strong>Associate Dragon clients with the Local Authenticator</strong></td>
</tr>
</tbody>
</table>
|                                                                      | See the "Configuring the Dragon Client for Nuance Management Center" chapter in the *Dragon Group Installation Guide*.
|                                                                      | This steps assumes you have already installed Dragon clients.           |

**On-premise NMC server**

If you're hosting your own NMC server on-premise, use this checklist to help you prepare for the configuration.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Create an NMC console administrator account for Active Directory</strong> on page 38</td>
</tr>
<tr>
<td></td>
<td><strong>Set the Active Directory connection string</strong> on page 39</td>
</tr>
<tr>
<td></td>
<td><strong>Create and configure user accounts in the NMC console</strong> on page 40</td>
</tr>
<tr>
<td></td>
<td><strong>Associate Dragon clients with the NMC server</strong></td>
</tr>
</tbody>
</table>
|                                                                      | See the "Configuring the Dragon Client for Nuance Management Center" chapter in the *Dragon Group Installation Guide*.
|                                                                      | This steps assumes you have already installed Dragon clients.           |
Creating an NMC console Administrator user for Active Directory

To configure Active Directory single sign-on and manage settings, you must create an Administrator user in the NMC console. You cannot use the initial NMC console login that Nuance provides (cloud NMC server), or the login that you create during the NMC console installation (on-premise NMC server). The Active Directory administrator login must match a login that exists in Active Directory.

1. Log in to the NMC console.
2. From the Menu bar, select User Accounts.
3. In the User Accounts ribbon, click the Add icon.
   The User Account Details window opens.
4. Configure the settings in the tabs:
   - Details—The highlighted text boxes indicate required data (First Name, Last Name and Login).
   - Address—Enter the user’s physical address.
   - Group Memberships—Add the Active Directory administrator to a Group.
   - Messaging: Configure email settings to enable the NMC console to send messages to users and administrators.
   - Dragon Professional—Configure user settings in the Dragon client.
     For now, you can skip this step. The default settings are applied. For more information, refer to “Configuring user settings” in the Nuance Management Center Administrator Guide.
   - User Profile—Ignore these settings. They are provided by the Dragon client.
5. Click Save.
   A dialog box appears, displaying the available licenses. If no administrator licenses are available, contact your Nuance representative.

After you have completed the steps above, log out of the NMC console, then log in using the NMC console administrator user account you created for the Active Directory administrator. You can now revoke the NMC console administrator license of the original admin user and grant that license to another user account.
Setting the Active Directory connection string

1. In the NMC console menu bar, click Sites, then click the Organization Overview icon. Click your organization, and then click the Details icon in the Organizations area.
   
   The Organization Details screen appears.

2. Click the Domains tab.

3. Click Add.
   
   The Domain dialog box appears.

4. Enter the following:
   
   **Name**—Your domain name. For example, ABCCompany.
   
   **Active Directory connection strings**—The Active Directory connection string. For example, LDAP://nuance.com.
   
   Ask your Active Directory domain administrator for the correct connection string. When Active Directory is enabled, Nuance Management Center sends all authentication requests to this server.

5. Click Save.

6. Repeat steps 3-5 as needed for each domain.
Creating and configuring user accounts for single sign-on

Creating user accounts

If you have not already created user accounts in the NMC console, you must create them before enabling single sign-on. When you create user accounts, each user’s login must match that user’s Windows domain login exactly.

On the User Account Details screen (click User Accounts in the menu bar, then click the Add icon), enter the user’s Windows domain login name in the Login field:

For example, enter "John_Doe" in the Login field if the user’s Windows domain login name is one of the following:

- “Domain\John_Doe”
- “John_Doe@domain.example.com”

Configuring user accounts

When you have created user accounts, do the following to add the users to your domain:

1. From the menu bar, click User Accounts.
2. Click Search to search for a user.
3. Specify search criteria, and then click Search.

   Search results appear.

4. Right-click a user, and then select User Account Details.
5. Click the Credentials tab.
6. Click the NTLM tab.
7. Click Add.

   The New NTLM Credential dialog box appears.

8. Select your domain from the Domain drop-down list.
9. Enter the user’s Windows domain login in the Login field.
10. Click Save.
Chapter 7: Installing the Local Authenticator

About the Local Authenticator ................................................................. 42
Local Authenticator logs ................................................................. 42
Downloading the Local Authenticator .................................................. 43
Creating organization tokens ......................................................... 44
Installing and binding the SSL certificate ................................................. 45
  About signed certificates ................................................................. 45
  Install the SSL certificate .............................................................. 45
  Testing and troubleshooting your SSL configuration ............................... 48
Installing the Local Authenticator ....................................................... 50
Editing the configuration file ............................................................. 54
Starting the Local Authenticator service ............................................... 55
About the Local Authenticator

The Local Authenticator is a service that provides Dragon clients with Active Directory single sign-on authentication. The Local Authenticator validates Dragon client credentials when the clients attempt to connect to the Nuance-hosted cloud NMC server, and then passes the validate credential call to the cloud NMC server to create a session.

You must install the Local Authenticator to use single sign-on with the Nuance-hosted cloud NMC server. You do not need the Local Authenticator if you’re hosting your own NMC server on-premise.

Install the Local Authenticator on a local server that is accessible to both the NMC server and your Dragon clients. You must have Administrator privileges on the server where you are installing the Local Authenticator.

For software system requirements for the Local Authenticator, see “Software requirements—Single sign-on for the Cloud NMC server” on page 36.

Local Authenticator logs

The Local Authenticator uses the same service trace logs as Nuance Management Center. These logs can be found in:

C:\ProgramData\NMS\Logs
Downloading the Local Authenticator

You can download the LocalAuthenticator.exe file from your NMC console. You then install the Local Authenticator on a local server that is accessible to both NMC server and your Dragon clients.

To download the Local Authenticator:

1. Log in to your NMC console as an Administrator.
2. In the Utilities ribbon, click **Tools**.
   
   The Tools page appears.
3. Click **Install local authenticator**.
   
   A message appears, prompting you to save or run the Local Authenticator executable.
4. Click **Save**.
   
   The LocalAuthenticator.exe file is saved to your local Downloads folder.
5. Copy the LocalAuthenticator.exe file to the local server on which you are installing it.
Creating organization tokens

The Local Authenticator installation requires an organization token. You create a token in the NMC console. To create an organization token:

1. From the menu bar, select Sites > Organization Overview.
2. Right-click your organization, and then select Details.
   The Organization Details page appears.
3. Click the Organization Token tab.
4. Click Add to generate a new organization token.
   The Organization Token Info dialog box appears. The Organization Token field is pre-populated with a system-generated token.
5. Optionally, enter a value in the Comment field.
6. Write down the token number.
   You must enter this number during the Local Authenticator installation.
7. Click Save.
   The new token appears in the Organization Token table.
Installing and binding the SSL certificate

About signed certificates

Using SSL requires that you obtain an SSL certificate. Nuance Management Center supports both signed certificates from a certificate authority, and self-signed (or internally generated) certificates. However, Nuance strongly recommends that you use a signed certificate, as self-signed certificates are not always easily recognized by the client the same way signed certificates are.

You can obtain signed certificates from certificate authorities, such as GoDaddy or Verisign. To obtain a signed certificate, you’ll need to provide information to the certificate authority about your organization and the server on which you are installing the certificate in the Certificate Signing Request (CSR). Each certificate authority may require different information. Typically, the information can include the following:

- Organization name
- Organization location information, such as town and state
- Computer name for the server on which you are installing the certificate
- Extended Key Usage value, such as 2.5.29.37. Extended key usage further refines key usage extensions, which define the purpose of the public key contained in the certificate.
- Key Size, such as 2048 bits or 4096 bits. Determines the length of the public key in the certificate. A longer key provides stronger security. You determine the level of security that is appropriate for your environment.

You obtain this information from your IT department, or from the person who installed and configured your server.

For more detailed information on installing SSL certificates, see:


Install the SSL certificate

Clients contact the Local Authenticator on the standard HTTP ports 80 and 443.

1. Install an SSL certificate in the Personal Store under the Local Computer section for the "logon as" user account under which the NMS service is running.

   To add the Certificates Snap-in and view the certificates installed on the local computer, see https://technet.microsoft.com/en-us/library/cc754431(v=ws.11).aspx.
2. Note the subject of the certificate.

This should match the computer name that the certificate is deployed on, or be a wild card. This must match exactly the host used in the endpoints. For information on viewing the subject, see https://technet.microsoft.com/en-us/library/cc754686(v=ws.10).aspx.
3. Copy the thumbprint of the certificate. You use the thumbprint to bind the certificate to the port used by the primary NMS services in the next step.

For information on retrieving the thumbprint, see https://msdn.microsoft.com/en-us/library/ms734695.aspx.

4. Bind the SSL port (443) used by the services to the certificate.

   **Windows Server 2008 or 2012:**
   
   a. Open a command prompt.
   
   b. Using the `netsh` utility, run the following command to bind port 443 to the certificate:

   ```bash
   netsh http add sslcert ipport=0.0.0.0:443 certhash=<thumbprint> appid={00000000-0000-0000-0000-000000000000}
   ```

5. Verify that the `UseSSL` setting is set to true (this should have been done by the installer):

   a. In `Nuance.NMS.Server.exe.config`, located in the NMS Platform installation folder, find the line near the top that contains the `key="UseSSL"` tag.
   
   b. Change the value to true:

   ```xml
   <add key="UseSSL" value="true"/>
   ```

6. Bind the SSL certificate under IIS to port 443.
a. In the IIS Manager, from the left panel, click **Default Web Site**.

b. From the right panel, click **Bindings**...

   The Site Bindings dialog box opens.

c. Click **Add**.

   The Add Site Binding dialog box opens.

d. From the **Type** drop-down list, select **https**.

e. From the **SSL certificate** drop-down list, select the certificate that you installed.

f. Click **OK**.

   The Site Bindings dialog box appears. Ensure that the binding is displayed correctly.

7. Restart the Local Authenticator server to allow any configuration changes to take effect.

**Testing and troubleshooting your SSL configuration**

- **Run these tests on a different computer. Do not run them on the Local Authenticator server.**

**Use the browser**

1. Can you access and log into the NMC console?
   a. Connect to https://<SERVER_NAME>/NMCHTML/.

   If you see the Nuance Management Center login page, port 443 is working, and the NMC console is being deployed properly.

   b. Log in to the NMC console. If successful, the console is able to communicate with the server.

2. Can you access the NMC console status interface?

   An XML response should appear in the browser.

3. Can you make RESTful web service calls?

   Attempt to create an NMS session using the browser.


   A prompt for a login and password appears.

   b. Use any valid NMC console login and password.

   c. If some XML is returned, the NMC console is configured properly and working with SSL.

4. Can you access the NMS API Help pages?

   b. Enter any credentials if prompted.

   c. An HTML page with help for one of the NMS API sets should appear. If you see this help, the NMS is configured and working properly.
Check the Bindings

If the NMC console is not working, ensure that the ports are properly bound to the SSL certificate. You can do this by using the "netsh http show ss1cert" command to display the current configuration. Be sure that port 443 is bound to the certificate.
Installing the Local Authenticator

On the server where you are installing the Local Authenticator:

1. Run the LocalAuthenticator.exe file.
   A dialog box appears, prompting you to select a language for the installation.
2. Select your language from the drop-down list, and then click OK.

   ![Image of InstallShield Wizard]

   The InstallShield Wizard opens.

3. Click Next.

   ![Image of InstallShield Wizard]

   Welcome to the InstallShield Wizard for the Local Authenticator
   The InstallShield Wizard will install Local Authenticator on your computer. To continue, click next.
4. Leave the default value in the **User Name** field, and enter your company name in the **Company** field. Then, click **Next**.

![Customer Information](image)

5. Set the location in which to install the Local Authenticator, and then click **Next**.

![Choose Destination Location](image)
6. In the **Token** field, enter the organization token that you generated in the NMC console, and then click **Next**.
7. Click **Install**.

8. When the installation is complete, the InstallShield Wizard Complete dialog appears. Click **Finish** to exit the installer.
Editing the configuration file

You edit the Local Authenticator configuration file to change the NMC server address to the appropriate address. You should have received this address in your welcome information from Nuance.

1. Open the folder where the Local Authenticator is installed. By default, the Local Authenticator is installed in:
   
   C:\Program Files\Nuance\Local Authenticator

2. In any text editor, open NMS.LocalAuthenticator.Service.exe.config.
   
   This is the Local Authenticator configuration file.

3. Find the line "<add key="NMSServerAddress" value="<NMS in the Cloud/>"/>" and change the value to the address of your NMC server.

4. Save your changes.
Starting the Local Authenticator service

1. Open the Server Manager to view your Windows services.
2. Look for the **NMS Local Authenticator Service**.
3. Right-click the service, and then select **Start**.
About database backups

If you are hosting your own NMC server on-premise, database backups occur on a regular basis at scheduled intervals automatically. The backup process places backup files in the C:\NMSDBBACKUP folder on the database server by default, unless you specified a different location during installation. The backup includes database objects, like sites and groups, and includes the Windows communication foundation service logs generated for each user account. Backups occur on the following schedule:

- **Transaction log backup**—Hourly
- **Differential database backup**—Daily at 2AM
- **Full database backups**—Weekly at 2AM

The database server retains one month of backups on disk. To retain more data, you must copy the files before the end of the month, when the backup process deletes files older than one month.

Disabling automatic database backups

Optionally, you can choose to disable the automatic backups and manage database backups yourself outside the Nuance Management Center. To disable automatic backups:

1. From the NMC menu button, select **System Settings**.
   
   The System Settings dialog box opens.

2. In the General section, select the **Disable scheduled NMS database backups** check box.

3. Click **Save**.